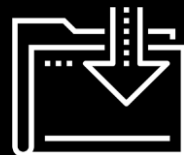




Risk Management and Threat Modeling

Cybersecurity
GRC Unit, Day 2



Class Objectives

By the end of today's class, you will be able to:



Identify threat agents, possible attacks, and exploitable vulnerabilities relevant to a given asset.



Prioritize risks based on likelihood and impact potential.



Choose and justify controls for a given risk.

Risk Management and Threat Modeling



What's the difference
between a vulnerability,
a threat, and a risk?



A **vulnerability** is an aspect of a business that can be exploited to compromise a system's CIA.



A **threat** is an actor that might exploit a vulnerability.



A **risk** is the possibility
of losing something valuable.

Risk Management And Threat Modeling

Risk Analysis

Understanding what risks face an organization, which are most severe, and which are most likely.

Risk Management

Using the results of risk analysis to create a plan for preventing likely risks.

Threat Modeling

Determining which attacks an organization is most likely to experience, who is most likely to launch them, and what actions can be done to prevent them.

Risk Management And Threat Modeling

What is a business's primary objective? **Profit!**



Risk analysis and management and **threat modeling** directly contribute to business profit.



Risk analysis helps business understand how much they'll need to spend in the event of a given security break.



When possible, risks are measured quantitatively in financial figures, which businesses use to prioritize threats.



Threat modeling results are shared upwards to the executives who make the major business decisions.

Threat Modeling Methodology: PASTA

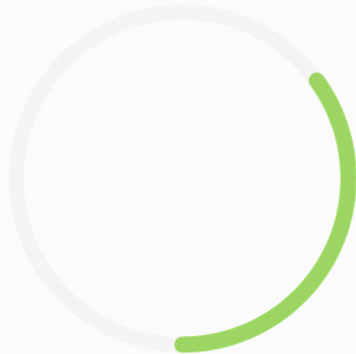
PASTA: **P**rocess for **A**ttack **S**imulation & **T**hreat **A**nalysis



PASTA focuses on aligning considerations of **business objectives** with **technical requirements**.

Threat Modeling Methodology: STRIDE

STRIDE: **S**poofing, **T**ampering, **R**epudiation, **I**nformation Disclosure, **D**oS (Denial of Service), **E**levation of Privilege



STRIDE focuses on identifying **what can fail** in the system being modeled.

Threat Modeling Methodology: OWASP

Today, we'll focus on OWASP

OWASP: **O**pen **W**eb **A**pplication **S**ecurity **P**roject

OWASP focuses on **identifying possible threats, prioritizing risks, and planning mitigation strategies**. It is mainly used with web and desktop applications.

OWASP

The **OWASP Threat Modeling process** consists of six steps.

1

Determine
assessment
scope

2

Identify
threat
agents

3

Identify
potential
attacks

4

Identify
exploitable
vulnerabilities

5

Prioritize
identified
risks


6

Mitigate
risks




Step 1 Determine Scope

List the assets under consideration, determine their value, and define objectives for your threat modeling assessment.



Businesses can't effectively evaluate everything at once, so they adjust their scope to focus on a specific category of risk.

Example: Performing a risk analysis to assess the weakness of a network infrastructure. Within this scope, we are not concerned with application security.



Scoping begins with asset inventory, the process of identifying and assigning asset value to all of an organization's assets.

Example: The asset value of a web application could be measured by the revenue or profit it generates.

Step 2 Identify Threat Agents

Determine which attackers would be interested in the relevant assets.

Threat agents include a person or group that can produce a threat, *whether or not* that person or group is malicious.

Threat agents include:

- APTs (Advanced Persistent Threats)
- Script kiddies
- Employees opening phishing emails
- Incompetent user breaking configurations on company computer



Today, we'll focus on *malicious* threat agents.

Previously in class, we addressed *unwitting* threat agents, like employees opening phishing emails.

Step 3

Identify Potential Attacks

Identify the attacks each agent is likely to perform.

Different attackers use different modes of attacks. Different attacks mean different risks and different considerations.

Example: Script kiddies will have different goals than a disgruntled employee.

We can identify a potential attack by considering the threat agent's:

- Motivation
- Skill level
- Amount of funding


Example: If a client's web application is taken offline by a DoS attack, the severity of the risk depends on which threat agent is responsible.

- Script kiddies might DoS a server simply to cause trouble.
- An APT might DoS a server as a smoke screen to steal valuable data.



Step 4 Identify Exploitable Vulnerabilities

Identify the most vulnerable points in a system, how the agent will deliver the attack, and where an attack is most likely to occur.



Once we determine who might attack and what methods they might use, we determine where exactly in the system they will likely direct their attacks, and what will be at risk if they do.

Example: If a network has only one database that stores everything, the entire company will lose access to all data if it is compromised. An attacker seeking to DoS the company's network can exploit this database to achieve their goal.



Activity: Threat Modeling: Steps 1-4

In this activity, you'll learn more about GeldCorp's business operations and assets before applying steps 1-4 of the OWASP process.

Instructions shared on Slack.

Suggested Time:
30 Minutes





Times Up! Let's Review.

Threat Modeling: Steps 1-4

Risk Analysis

Risk Analysis

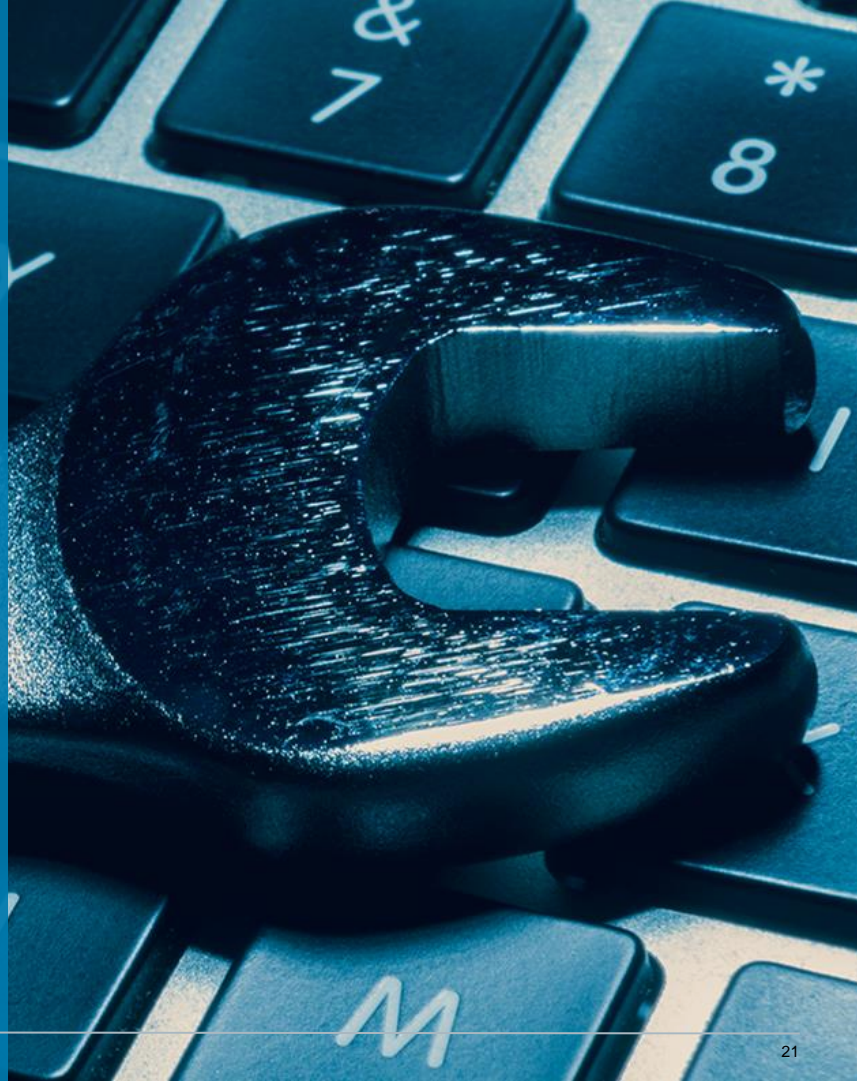
Risk analysis is the process of prioritizing threats identified in steps 1-4 based on their potential impact and likelihood.

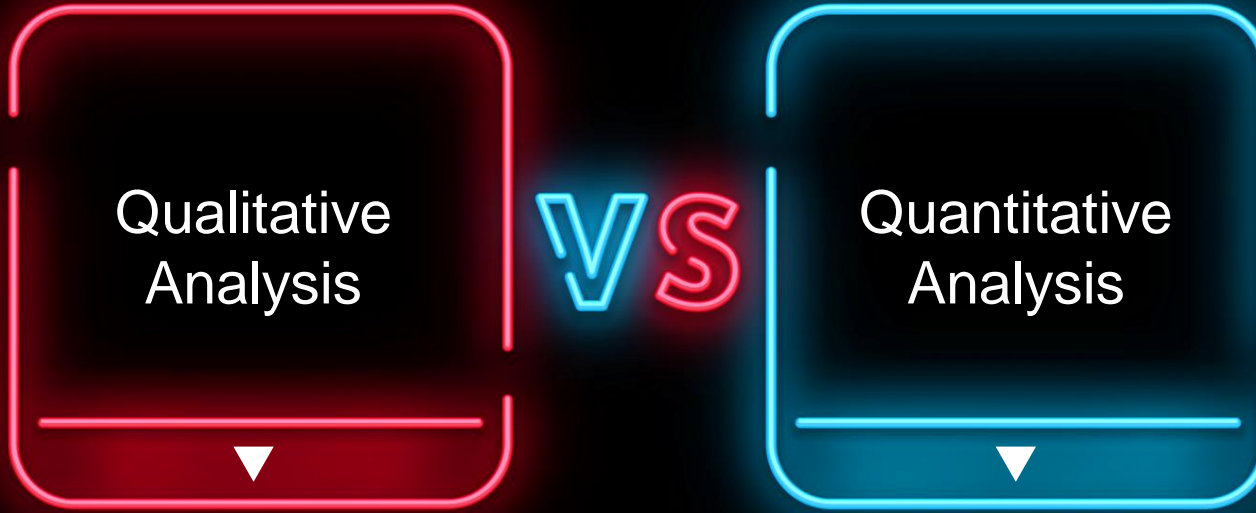
Scenario

You've identified more than 10 potential attacks that GeldCorp should consider. All can be mitigated, but each fix costs around \$2.5k. GeldCorp's Security Department only has \$10k budgeted for the project. You must provide guidance on which four fixes should be prioritized.

Before completing this activity, we'll learn about:

- Qualitative vs. Quantitative Risk Analysis
- Likelihood, Impact, and Loss Expectancies
- Risk Factor and Heat Maps





- Evaluating risk based on intangible, unmeasurable factors.
 - Used when analysis leads to decisions without the need of cost-benefit analysis.
- Evaluating each risk based on its measured likelihood and impact.
 - **Likelihood:** The probability an event will take place.
 - **Impact:** The measure of damage done if a risk takes place.

Qualitative Risk Analysis



In some situations, likelihood and impact cannot be accurately measured.

- **Example 1:** It's impossible to calculate the precise probability that some lone attacker, somewhere in the world, will attack your servers within the next year.
- **Example 2:** It's impossible to determine the precise impact of a breach. The cost of an attack will depend on its length, which is impossible to determine ahead of time.

Qualitative Risk Analysis

- Used when a complex evaluation of cost vs. benefit is unnecessary.

Example: When a company is deciding between an inexpensive VPN service that logs traffic on its servers for internal use, and a more expensive service that does not keep any logs.



A **bakery** can use qualitative analysis to decide on an inexpensive VPN, since it shouldn't matter much if they're logging non-confidential information.



A **government defense or financial organization** can use qualitative analysis to decide on a more expensive service, since it knows it needs to keep its data confidential.

Quantitative Risk Analysis: Example 1



However, there are circumstances where intuitive analysis is insufficient.

- **Example:** The Security Department wants to invest in protecting the organization's infrastructure.

In order to secure the money from the Finance Department, they must justify their ask. They present a quantitative risk analysis to demonstrate that the cost of not investing is much greater than the budget they're requesting.

Quantitative Risk Analysis: Example 2



However, there are circumstances where intuitive analysis is insufficient.

- **Example:** The Executive Team must decide whether to migrate to a new cloud provider as part of negotiations with a potential partner.

This transition has major financial implications. To make the decision, they need an accurate assessment of potential losses due to downtime, retraining, risk of data corruption during migration, and other issues.

Asset Value and Exposure Factor

To perform quantitative risk analysis, analysts start by calculating how much it will cost if an asset is breached.



They first quantify **asset value** and **exposure factor**.



As discussed earlier, **asset value** is how much money an asset is worth in currency.



The **exposure factor** is how much of an asset will be affected in the event of a breach.



In other words, will an attack result in **partial / temporary** or **complete / permanent** destruction of an asset.

Determining Exposure Factor

Exposure factor is always somewhat subjective. We apply a numerical value depending on the level of damage an exploited risk would produce.

1.0

Attack would **completely eliminate** an asset.

.75

Attack would **mostly eliminate** an asset.

0.5

Attack would **half eliminate** an asset.

.25

Attack would **partially eliminate** an asset.

Loss Expectancy

The measure of how much money an organization will lose in the event of a given breach.

Single Loss Expectancy (SLE)

Estimated cost of the risk occurring on a given asset.

$$\text{SLE} = \text{AVE} \times \text{EF}$$

AV = Asset Value

EF = Exposure Factor

Annual Rate of Occurrence (ARO)

Estimated number of times the risk is likely to occur in a given year.

Annual Loss Expectancy (ALE)

Estimated cost of a risk occurring in a given year.

$$\text{ALE} = \text{SLE} \times \text{ARO}$$

Loss Expectancy

Categories of loss expectancy refer to the degree of a breach's impact.

Marginal

The organization has the resources to respond to the breach immediately, without affecting day-to-day operations or revenue.

Notable

The organization has the resources to respond to the breach, but may not be able to do so immediately. May experience interruptions to operations.

Severe

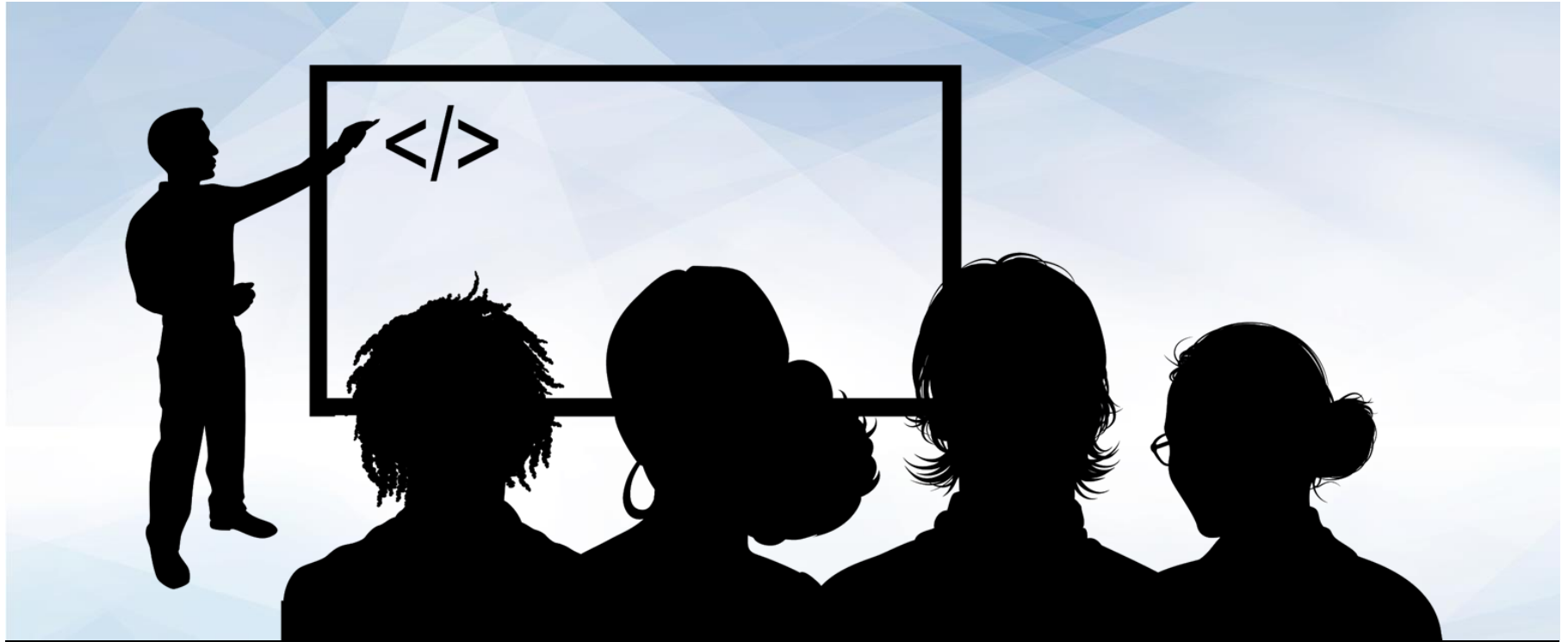
The organization experiences serious interruptions to operations, and doesn't have the monetary and/or personnel resources to respond to effectively. May have to defer revenue, delay project timelines, reassign employees, and/or hire consultants to address the issue.

Catastrophic

The organization suffers severe, lasting damage to its reputation and/or infrastructure. The future of the business is threatened by reputational damage, bankruptcy, being found in contempt of federal regulations, or other issues.



In the next demonstration,
we'll see data presented in
spreadsheet and visual formats
through **risk matrices and heat
maps.**



Instructor Demonstration

The Risk Spreadsheet





Countdown timer

15:00

(with alarm)



Activity: Threat Modeling

Step 5 - Risk Analysis

In this activity, you will complete a spreadsheet and generate a risk matrix and heat map for GeldCorp.

(Instructions sent via Slack.)

Suggested Time:
30 Minutes





Times Up! Let's Review.

Threat Modeling: Step 5 - Risk Analysis

Mitigating Risks



Now that we're able to determine which threats are worth our attention and resources, we can craft controls for mitigating risks.

Deciding on Security Controls

Answer the following questions when determining an appropriate control.



Should the control be physical, administrative, or technical? **(Required Control Type)**



How strong does the control *really* need to be? **(Required Strength of Control)**



How much does the control cost compared to the benefit provided?
(Cost of Implementation)



How long will the control take to implement? **(Time of Implementation)**

Risk Mitigation: Example

LifeNotes is a new medical records company that makes it easy for doctors from different hospitals to share medical records.

When transferring a patient to another hospital or physician, they can use the application to share the patient's medical history, lab results, and medication schedules.

LifeNotes also ensures that doctors can only see records for their own patients.

However, a client recently reported that they were able to load records for patients they were not assigned to.

This violates regulatory standards protecting patient medical information, and must be resolved immediately.



Risk Mitigation: Example

What security controls should we suggest to LifeNotes?

- Required Control Type?
- Required Control Strength?
- Control Decisions?
- Cost of Implementation?
- Time of Implementation?





Activity: Threat Modeling Step 6 - Risk Mitigation

In this activity, you will conceptualize a risk mitigation plan.

Instructions shared on Slack.

Suggested Time:
15 Minutes





Times Up! Let's Review.

Threat Modeling Step 6 - Risk Mitigation

Class Objectives

By the end of today's class, you will be able to:



Identify threat agents, possible attacks, and exploitable vulnerabilities relevant to a given asset.



Prioritize risks based on likelihood and impact potential.



Choose and justify controls for a given risk.

Practical Threat Modeling

IMPORTANT CONCEPTS

- ☐ Golden Question(s)
- ☐ Data Flow Diagrams
- ☐ Attack Trees
- ☐ Trust Boundaries
- ☐ STRIDE
- ☐ Secure Coding



GOLDEN QUESTIONS

- ☐ What are we working on?
- ☐ What can go wrong?
- ☐ What are we going to do about it?
- ☐ Did we do a good job?

- Adam Shostack

What are we working on?

- **New Feature**
- **Complex Application**
- **New Architecture**

What can go wrong?

- **S.T.R.I.D.E**
- **Cyber Kill Chain**
- **Attack Speculation (A.K.A. Brainstorm)**

What are going to do about it?

- **Apply Security Controls**
- **Implement Mitigation**
- **Run Test Cases**

Did we do a good job?

- **QA Testing**
- **Pentest!**

BATMAN THREAT MODEL

ASSETS

THREATS



CONTROLS

- LOW RISK
- MED RISK
- HIGH RISK

BATMAN THREAT MODEL

ASSETS

Secret Identity

Batcave

Batmobile

Bat Phone

Alfred



CONTROLS

THREATS

- LOW RISK
- MED RISK
- HIGH RISK

BATMAN THREAT MODEL

ASSETS

Secret Identity

Batcave

Batmobile

Bat Phone

Alfred



CONTROLS

THREATS

Super Villains

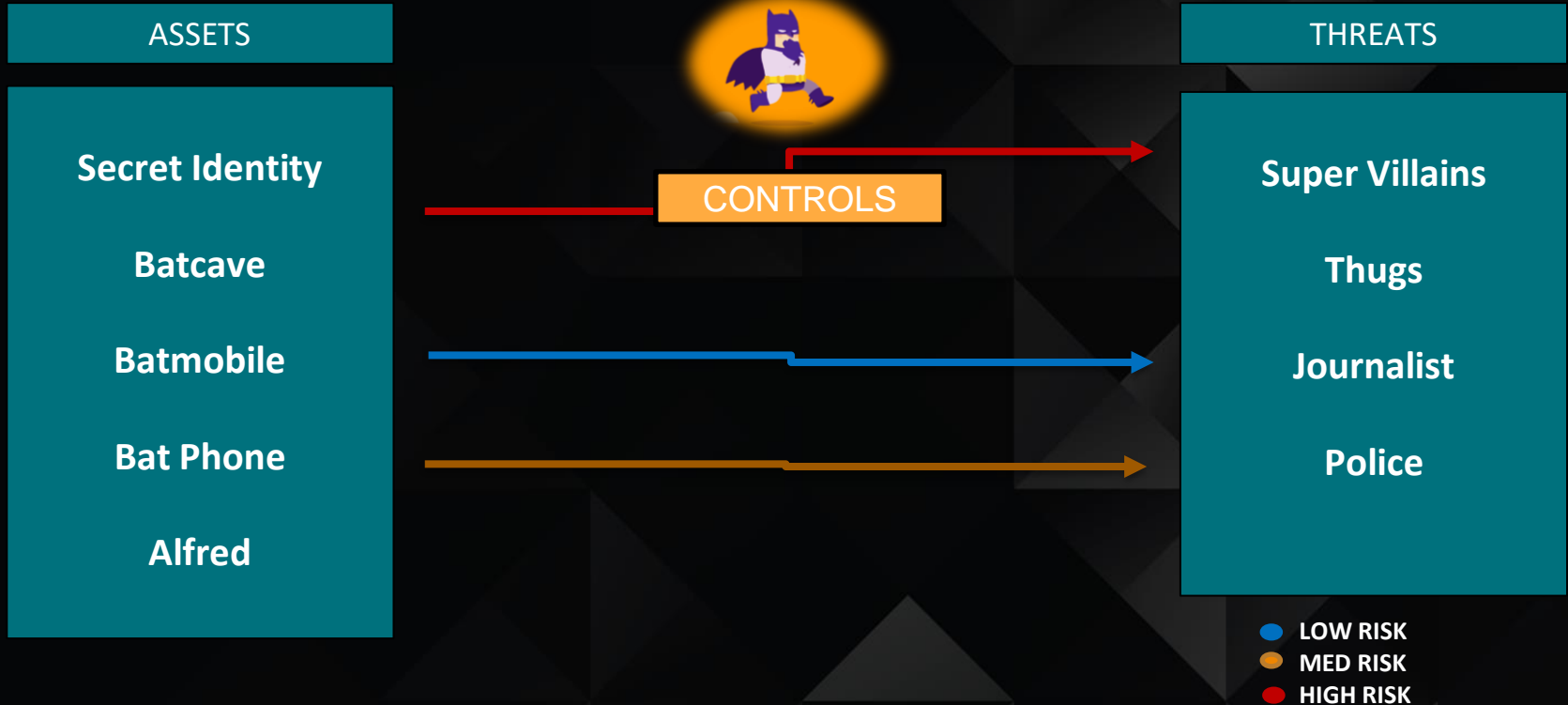
Thugs

Journalist

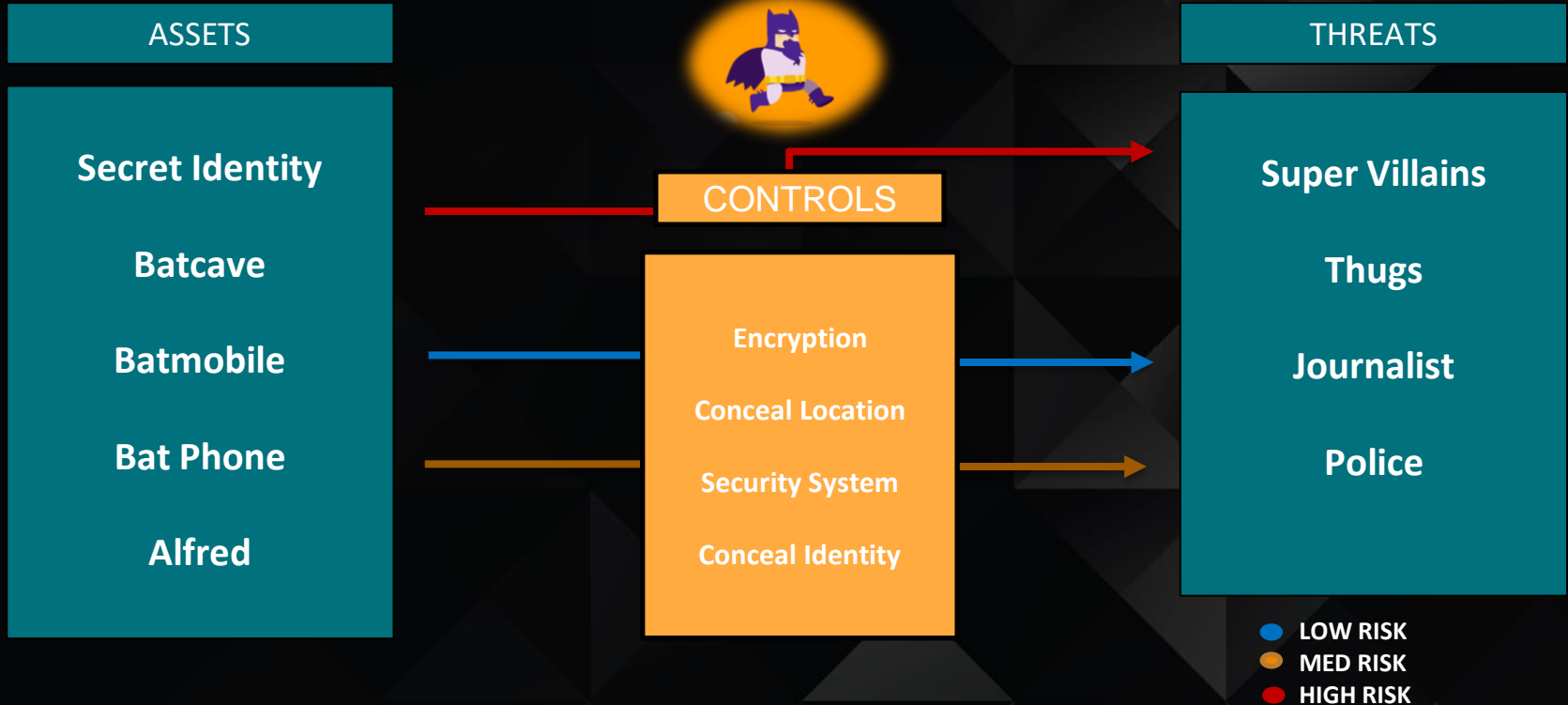
Police

- LOW RISK
- MED RISK
- HIGH RISK

BATMAN THREAT MODEL



BATMAN THREAT MODEL



TRUST BOUNDARIES

“Define any distinct boundaries (External boundaries and Internal boundaries) within which a system trusts all sub-systems (including data).”

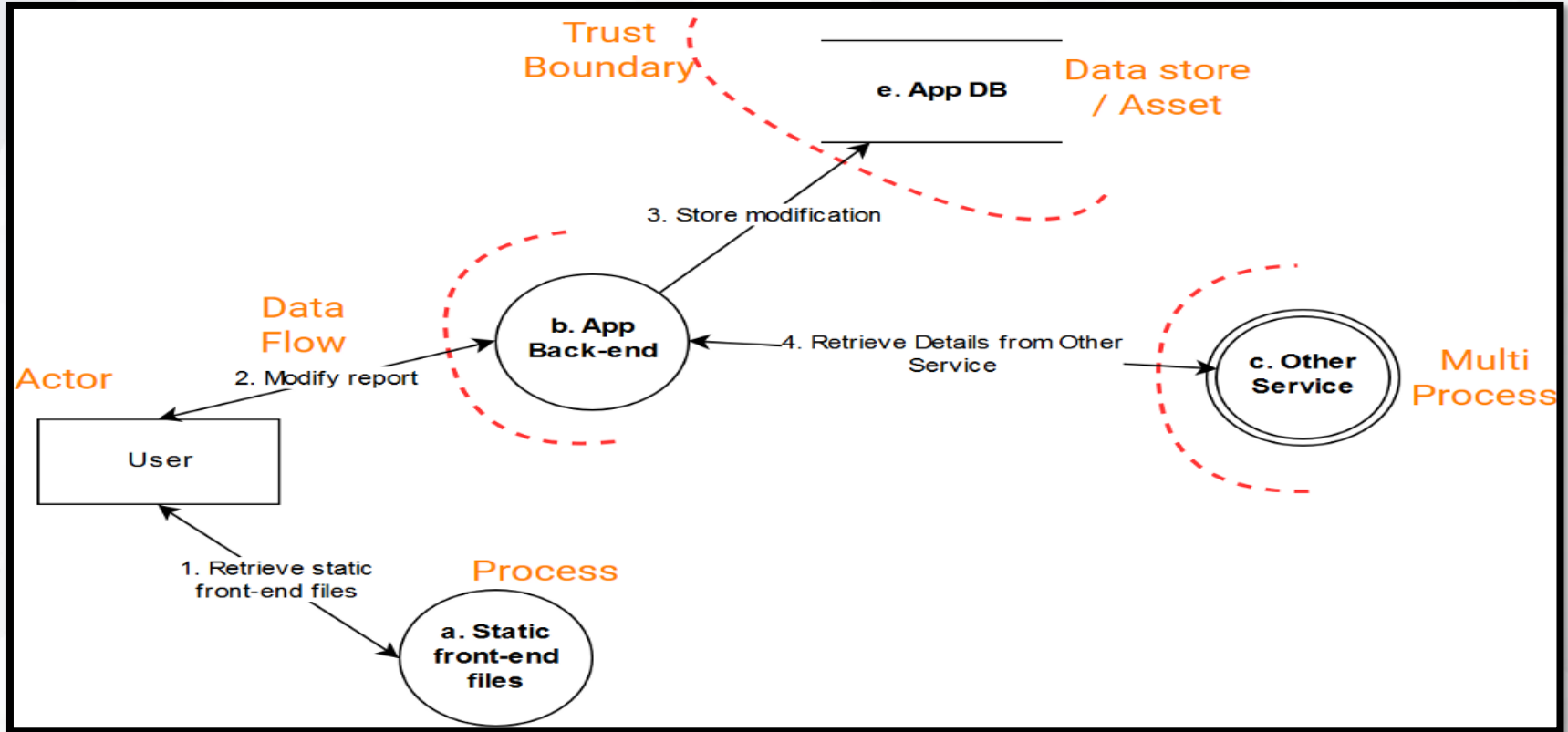
HOW TO:

- Identify each object on the data flow diagram
- Map where external data is processed by internal resources

SUCCESS TIPS:

- Map Data to Processes
- Know what you control and define the extent of that control

Data Flow Diagrams



S.T.R.I.D.E

Security property	Threats	
Authentication	Impersonate the Programmer Impersonate the IMD Impersonate the external device	Spoofing
Integrity	Patient data tampering Malicious inputs Modify communications	Tampering
Non-repudiation	Delete access logs Repeated access attempts	Repudiation
Confidentiality	Disclose medical information Determine the type of IMD Disclose the existence of the IMD Track the IMD	Information disclosure
Availability	Drain the battery of the IMD Interfere with the IMD communication capabilities Flood the IMD with data	Denial of service
Authorization	Reprogram the IMD Update the therapy of the patient Switch-off the IMD	Elevation of privileges

ATTACK TREE

SCENARIO #1: BATCAVE (SUPER VILLIAN)

OBJECTIVE

FIND BATCAVE

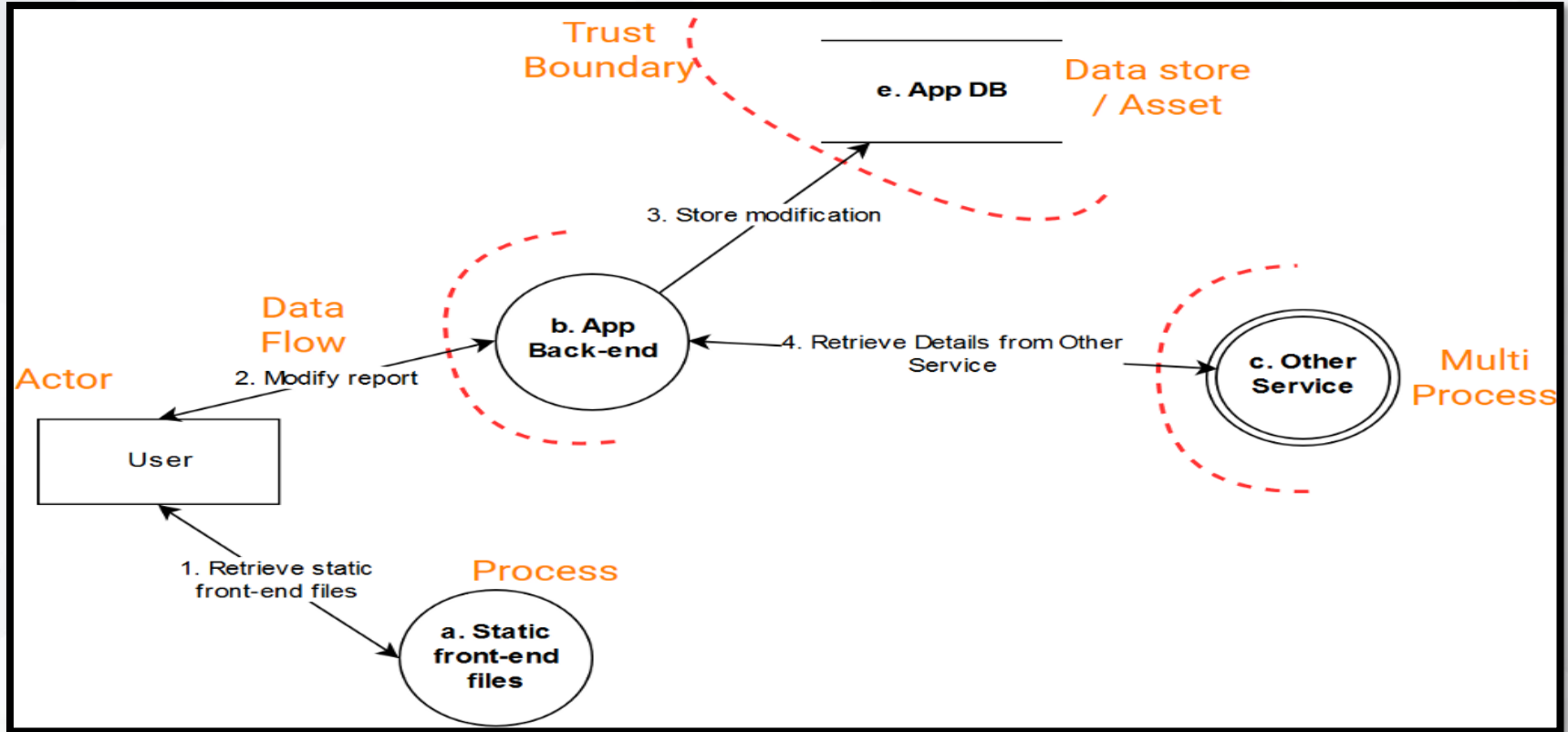
METHOD

FOLLOW
PLACE TRACKER
HIDE IN
BATMOBILE

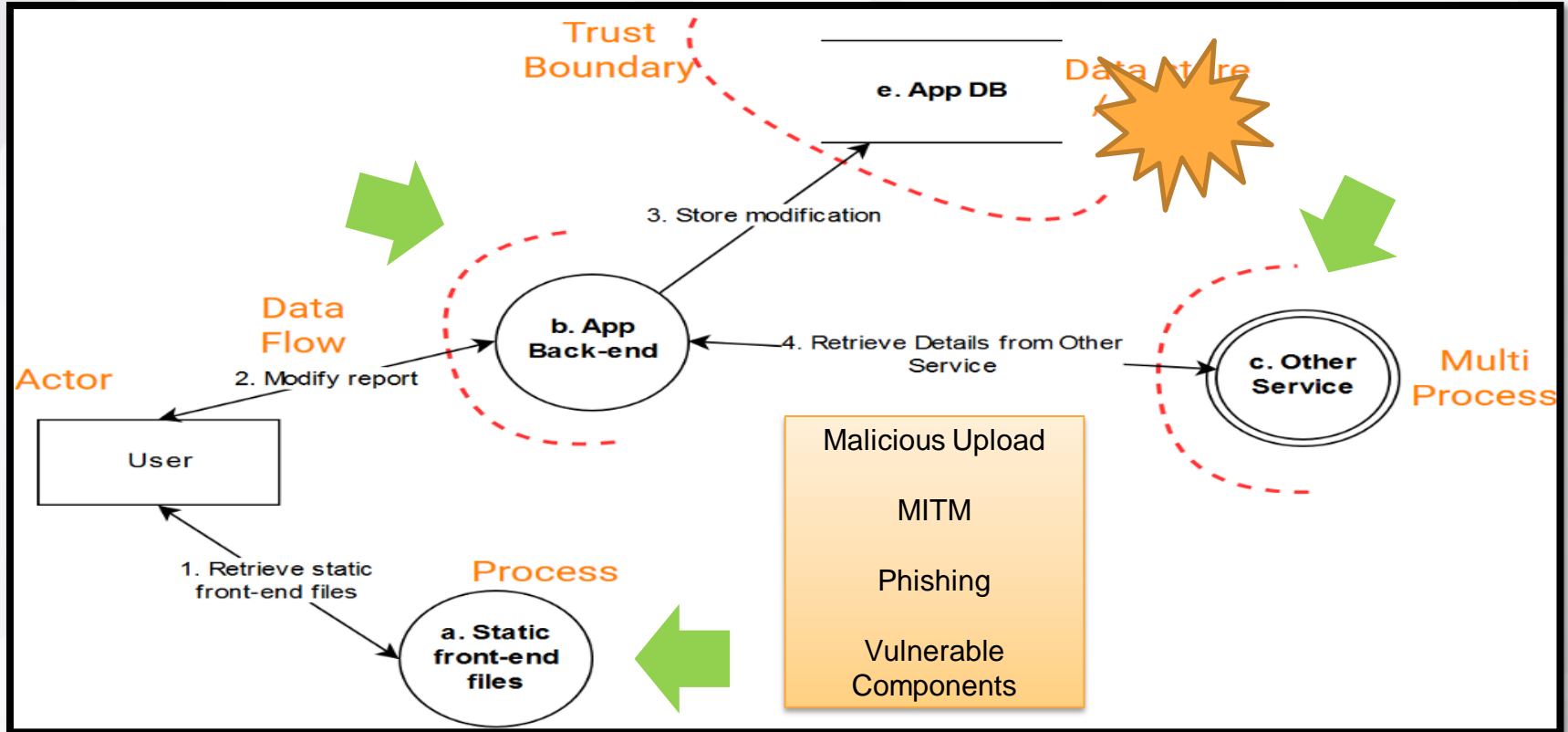
THREAT AGENT



APPLICATION: ATTACK TREE



APPLICATION: ATTACK TREE



SECURE CODING PRACTICES

In-depth Knowledge of language and potential vulnerabilities of faulty implementation for both logical and technical security issues.

Problem:

- Developers Write Insecure Code
- Dependencies are vulnerable

Solutions:

- Automated Tools: SAST and DAST Scanners
- Manual Secure Code Review

```
void launch_missiles(int n)
{
    printf("Launching %d missiles\n", n);
    // TODO: implement this function
}

void authenticate_and_launch(void)
{
    int n_missiles = 2;
    bool allowaccess = false;
    char response[8];

    printf("Secret: ");
    gets(response);

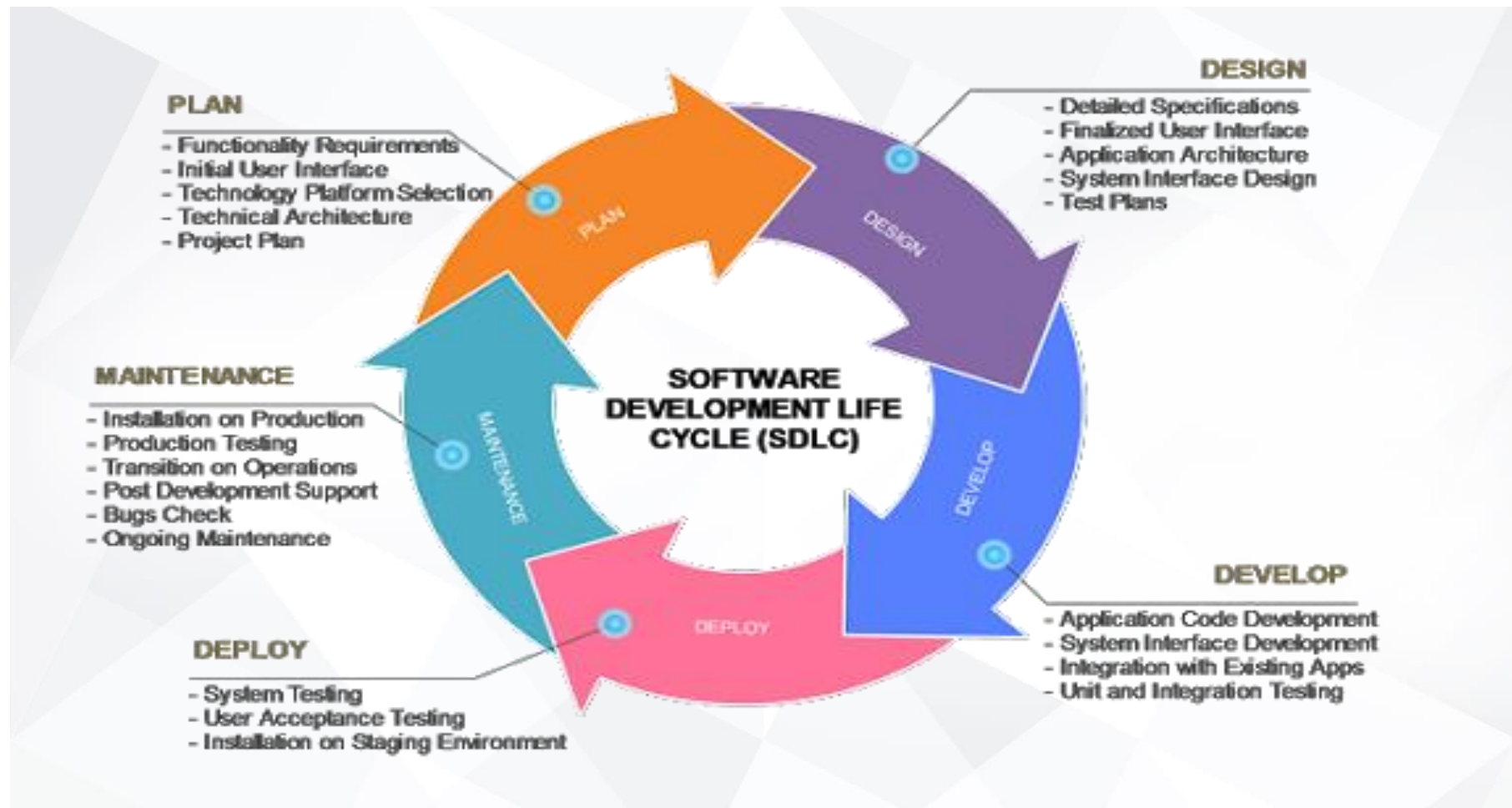
    if (strcmp(response, "Joshua") == 0)
        allowaccess = true;

    if (allowaccess) {
        puts("Access granted");
        launch_missiles(n_missiles);
    }

    if (!allowaccess)
        puts("Access denied");
}

int main(void)
{
    puts("WarGames MissileLauncher v0.1");
    authenticate_and_launch();
    puts("Operation complete");
}
```





LET'S MODEL THIS!

